Entanglement verification for quantum key distribution systems with an underlying bipartite qubit-mode structure

Johannes Rigas[1], Otfried Gühne[2] and Norbert Lütkenhaus[1]
[1] *Quantum Information Theory Group, Institut für Theoretische Physik I, and Max-Planck Research Group, Institute of Optics, Information and Photonics, Universität Erlangen-Nürnberg, Staudtstraße 7/B2, 91058 Erlangen, Germany*
[2] *Institut für Quantenoptik und Quanteninformation, Österreichische Akademie der Wissenschaften, A-6020 Innsbruck, Austria*
(Dated: February 1, 2008)

We consider entanglement detection for quantum key distribution systems that use two signal states and continuous variable measurements. This problem can be formulated as a separability problem in a qubit-mode system. To verify entanglement, we introduce an object that combines the covariance matrix of the mode with the density matrix of the qubit. We derive necessary separability criteria for this scenario. These criteria can be readily evaluated using semidefinite programming and we apply them to the specific quantum key distribution protocol.

PACS numbers: 03.67.Dd, 03.65.Ud, 03.67.Mn

I. INTRODUCTION

Quantum key distribution (QKD) protocols typically distinguish two phases: In the first phase, a physical apparatus is used to establish correlated data between the sender (called Alice) and the receiver (called Bob). This data are described by a joint probability distribution. In the second phase the data are processed by classical communication via an authenticated public channel employing methods such as post-selection, error correction and privacy amplification to distill a secret key (for a review see [1]).

A necessary precondition for the success of Phase II, i.e., for obtaining a secret key, is that the correlations in the data show signatures from quantum entanglement [2]. This means that the data must originate from an effective entangled state (effective, since the quantum state is not shared any more). Whenever only partial information on the whole bipartite state is available from the data, it means that all possible states compatible with the measurement outcomes must be entangled. If there is a separable state consistent with the data, then the QKD protocol is not secure.

For this, it makes no conceptual difference whether the entangled state is first distributed by an untrusted third party Eve before Alice and Bob perform the measurements on the state (so-called *entanglement-based* schemes, EB, see e.g. [3]) or whether Alice prepares an entangled state first, measures her part before sending the other part through the insecure domain under Eve's control to Bob, who performs his measurements (so-called *prepare&measure* schemes, PM, see e.g. [4, 5]).

The investigation of entanglement in QKD protocols using discrete variables, mainly qubits, was considered before for various protocols [2, 6]. For the case where Alice and Bob both control a continuous variable system, this issue has been addressed in Refs. [7, 8]. In this paper, we study this problem for the case where Alice owns a discrete system, namely a qubit, and Bob owns a mode.

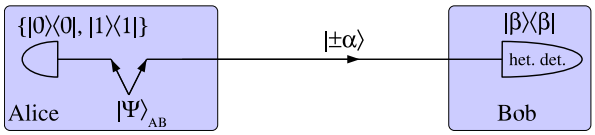

FIG. 1: (color online) In the considered QKD scheme Alice effectively sends two coherent states $|\pm\alpha\rangle$ to Bob, who performs heterodyne measurement, e.g. a projection onto coherent states. Alice's state preparation can be thought of as coming from an initial entangled state, as described in the text.

The protocol we investigate is described as follows (see Fig.1): Alice prepares the entangled state

$$|\Psi\rangle_{AB} = \sqrt{p_0}\,|0\rangle_A \otimes |\alpha\rangle_B + \sqrt{p_1}\,|1\rangle_A \otimes |-\alpha\rangle_B \qquad (1)$$

at her site. By projecting the state $|\Psi\rangle\langle\Psi|_{AB}$ either onto $|0\rangle\langle 0|_A$ or onto $|1\rangle\langle 1|_A$, Alice effectively sends coherent states $|\pm\alpha\rangle_B$ with *a priori probabilities* p_0, p_1 to Bob. The overlap of those input states is significantly larger than zero. Since Alice keeps her part of the state, her reduced density matrix

$$\rho_A := \mathrm{Tr}_B(|\Psi\rangle\langle\Psi|_{AB}) = \begin{bmatrix} p_0 & \sqrt{p_0 p_1}\langle -\alpha|\alpha\rangle \\ \sqrt{p_0 p_1}\langle\alpha| -\alpha\rangle & p_1 \end{bmatrix} \qquad (2)$$

is fixed.

After passing through the insecure domain controlled by Eve, Bob receives these states which may have changed, in particular affected by loss and noise, and he measures the covariance matrix of them, for instance by performing heterodyne detection. The states Bob receives conditioned on which state was sent by Alice are labeled with ρ_0 and ρ_1. After the measurements, the data are processed by classical communication in order to obtain a secret key.

This protocol is similar to the one proposed and implemented in [9] with the difference that in Ref. [9] also a strong phase reference, which is necessary for heterodyne detection as a local oscillator, has been sent from Alice to Bob. Since Eve may also access this phase reference, the security analysis for a practical setup is more complicated compared with the protocol described above.

The structure of this paper is as follows: With a simplified example, in Section II we outline that the key idea behind our approach is that the outcome states measured by Bob are very pure. In Section III, we introduce a description of qubit-mode systems which includes all information on the bipartite state accessible with heterodyne detection. We note some basic properties of this description and derive a necessary criterion for separability. In Section IV these conditions are applied to the special case of limited knowledge on the whole state in a PM scheme. Finally, a sufficient entanglement criterion is implemented numerically where the performance of the criterion is discussed with help of an explicit example.

II. BASIC IDEA BEHIND ENTANGLEMENT DETECTION

Let us explain the main idea for our entanglement detection scheme in a simple example. To that aim we will show no separable state can be compatible with the data if both conditional states ρ_0, ρ_1 are pure.

So let us assume that Bob receives two non-orthogonal, non-identical pure states, i.e., $\rho_i = |\varphi_i\rangle\langle\varphi_i|$, $i = 0, 1$, and $0 < \mathrm{Tr}(\rho_0\rho_1) < 1$. In this case, we can describe the whole bipartite state ρ_{AB} as

$$\rho_{AB} = \left[\begin{array}{c|c} p_0\rho_0 & C^\dagger \\ \hline C & p_1\rho_1 \end{array}\right], \tag{3}$$

with the pure states ρ_i completely known due to the tomographical completeness of Bob's heterodyne measurement and two arbitrary matrices $C, C^\dagger$ of which only the trace is known since $\mathrm{Tr}(C) = (\rho_A)_{10} = \sqrt{p_0 p_1}\langle\alpha| - \alpha\rangle$.

The two pure states $|\varphi_i\rangle$ span Bob's Hilbert space, so we can write down the matrix blocks in Eq.(3) in the eigenbasis of ρ_0:

$$\rho_{AB} = \left[\begin{array}{cc|cc} p_0 & 0 & c_{00}^* & c_{10}^* \\ 0 & 0 & c_{01}^* & c_{11}^* \\ \hline c_{00} & c_{01} & \multicolumn{2}{c}{\multirow{2}{*}{$p_1\rho_1$}} \\ c_{10} & c_{11} & & \end{array}\right]. \tag{4}$$

In this representation we can easily implement the constraint that ρ_{AB} is positive. Namely, this implies that $|c_{01}| = |c_{11}| = 0$, since the element $(\rho_{AB})_{22}$ on the diagonal is zero [10].

Under the assumption of separability of ρ_{AB}, also its partial transpose must be positive [11, 12]. Performing the partial transposition leads to the conclusion, that for PPT states also $|c_{10}| = 0$ has to hold.

For separable states we have therefore in the eigenbasis of ρ_0

$$\rho_{AB} = \left[\begin{array}{cc|cc} p_0 & 0 & S & 0 \\ 0 & 0 & 0 & 0 \\ \hline S & 0 & \multicolumn{2}{c}{\multirow{2}{*}{$p_1\rho_1$}} \\ 0 & 0 & & \end{array}\right], \tag{5}$$

with S abbreviating $\mathrm{Tr}(C) = \sqrt{p_0 p_1}\langle\alpha| - \alpha\rangle = \sqrt{p_0 p_1}\, e^{-2|\alpha|^2}$.

Similar arguments apply if we consider the eigenbasis of ρ_1 which is related to the eigenbasis of ρ_0 by a unitary matrix U. The transformed matrix $(\mathbb{1}_A \otimes U)\rho_{AB}(\mathbb{1}_A \otimes U^\dagger)$ must be of a form similar to (4). Then, by comparison of the off-diagonal blocks one obtains the equality

$$\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} = U \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} U^\dagger, \tag{6}$$

which implies that U is diagonal in the chosen basis with some complex entries on the diagonal of modulus one. From this it follows that $|\varphi_1\rangle = e^{i\lambda}|\varphi_0\rangle$, $\lambda \in \mathbb{R}$, which was excluded in the beginning. So we have derived a contradiction to the assumption of separability simply by making use of the purity of the states measured at B and the knowledge of the reduced density matrix ρ_A.

In the following, we will extend this idea to the case of outcome states which are affected by noise [29]. To this aim, we first need an adequate and powerful description of quantum states of a qubit and a mode. In the next Section we will introduce the so-called expectation value matrix for this task. Then, we will formulate separability criteria in this description. With these criteria, we can then investigate the presence of entanglement in the actual QKD protocol.

III. CLASSIFICATION OF THE EXPECTATION VALUE MATRIX

In our protocol, the density matrix has a special structure. While Alice has a discrete system, Bob's system consists of a continuous variable system, namely a mode.

On the one hand, there exist efficient operational entanglement criteria for bipartite discrete systems considering the system's density matrix [11–15]. On the other hand, criteria for bipartite CV systems exploiting uncertainty relations [16] and covariance matrices [17–19] of quadrature operators measured on the whole state are known.

One might be tempted to employ these CV entanglement criteria for our half-discrete, half-continuous problem (e.g. by describing Alice's discrete subsystem in terms of two Fock states with different photon numbers). However, it has been shown in Ref. [20] that these criteria can not be successfully applied here, due to the limited knowledge on the whole bipartite state in our PM scheme.

Therefore, we introduce in this section a quantity that describes the two different systems in their standard ways

and includes all properties accessible in a PM scheme using heterodyne detection. Additionally, the basic properties of this object are derived.

A. Definition

We introduce the *bipartite expectation value matrix* (EVM) $\chi \in \mathbb{C}^{6\times 6}$ as

$$\chi := \begin{bmatrix} \Big\langle |0\rangle\langle 0| \otimes B \Big\rangle & \Big\langle |0\rangle\langle 1| \otimes B \Big\rangle \\ \Big\langle |1\rangle\langle 0| \otimes B \Big\rangle & \Big\langle |1\rangle\langle 1| \otimes B \Big\rangle \end{bmatrix} \tag{7}$$

with B being the operator-valued matrix

$$B := \begin{bmatrix} \mathbb{1} & x & y \\ x & x^2 & \mathcal{S}(xy) \\ y & \mathcal{S}(xy) & y^2 \end{bmatrix}. \tag{8}$$

In this definition, x and y denote the quadrature operators, obeying the commutation relations $[x, y] = xy - yx = i$. Furthermore, $\mathcal{S}(xy)$ denotes the symmetrized product $(xy + yx)/2$ and $\langle A \otimes B\rangle = Tr(\rho A \otimes B)$ denotes the matrix of expectation values of the tensor product of A with all operators of B in a given state ρ_{AB}.

We take Alice's natural basis $\{|0\rangle, |1\rangle\}$ so that along with the identity on Bob's side, the elements of the reduced density matrix ρ_A are included (see next section). The two projectors $|0\rangle\langle 0|$ and $|1\rangle\langle 1|$ ensure that conditional quadrature expectation values and moments easily accessible to Bob are involved.

Explicitly, with the definitions (7) and (8) and the specific form of ρ_{AB} (3), the upper left 3×3-block in (7) becomes

$$\Big\langle |0\rangle\langle 0| \otimes B \Big\rangle = p_0 \begin{bmatrix} 1 & \langle x\rangle_0 & \langle y\rangle_0 \\ \langle x\rangle_0 & \langle x^2\rangle_0 & \langle \mathcal{S}(xy)\rangle_0 \\ \langle y\rangle_0 & \langle \mathcal{S}(xy)\rangle_0 & \langle y^2\rangle_0 \end{bmatrix} =: p_0\, \eta_0, \tag{9}$$

with the expectation value $\langle b\rangle_0 := \mathrm{Tr}(b\rho_0)$, defining η_0 as the *single mode's* EVM of the state ρ_0. Obviously, η_0 is real and symmetric by construction.

B. Properties

We now want to derive properties of the EVM η_0 of ρ_0. For this, let us first look at the covariance matrix γ_0 of a single mode, defined as

$$\gamma_0 := \begin{bmatrix} \Delta(x)_0 & \Delta(\mathcal{S}(xy))_0 \\ \Delta(\mathcal{S}(xy))_0 & \Delta(y)_0 \end{bmatrix} \tag{10}$$

with $\Delta(x)_0 = \langle x^2\rangle_0 - \langle x\rangle_0^2$ and $\Delta(\mathcal{S}(xy))_0 = \langle \mathcal{S}(xy)\rangle_0 - \langle x\rangle_0\langle y\rangle_0$ etc. For such a matrix, it is known that a necessary and sufficient criterion of being a covariance matrix of a physical state is

$$\gamma_0 + \frac{i}{2}J \;\geq\; 0 \text{ with } J = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}. \tag{11}$$

This condition is an implementation of the canonical commutation relations and the resulting uncertainty relations obeyed by x and y [21, 22]. Note that complex conjugation of Eq. (11) yields $\gamma_0 - \frac{i}{2}J \geq 0$, hence $\gamma_0 \geq 0$ has to hold, too.

Now we will show that for η_0 a condition similar to Eq. (11) holds, namely

$$\left(\eta_0 + \frac{i}{2}\tilde{J}\right) \geq 0 \text{ with } \tilde{J} := \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & 1 & 0 \end{bmatrix}. \tag{12}$$

Indeed, using the commutation relations $[x, y] = i$ one can see that

$$\eta_0 + \frac{i}{2}\tilde{J} = \begin{bmatrix} \langle \mathbb{1}\rangle_0 & \langle x\rangle_0 & \langle y\rangle_0 \\ \langle x\rangle_0 & \langle x^2\rangle_0 & \langle yx\rangle_0 \\ \langle y\rangle_0 & \langle xy\rangle_0 & \langle y^2\rangle_0 \end{bmatrix}, \tag{13}$$

which is clearly positive since any term $\vec{s}^\dagger(\eta_0 + i\tilde{J}/2)\vec{s}$ with $\vec{s} = (s_1, s_2, s_3)^T$ can be expressed as $\langle A^\dagger A\rangle$ with $A = s_1 + s_2 x + s_3 y$.

Obviously, the positivity condition (12) does not depend on a particular measurement on Alice's side but must hold for any projector $|s\rangle\langle s|$ evaluated by A, i.e., for any $\rho_s := \mathrm{Tr}_A(\rho_{AB}|s\rangle\langle s| \otimes \mathbb{1})$, the corresponding EVM η_s must fulfill $(\eta_s + i\tilde{J}/2) \geq 0$.

Furthermore, from Eqs. (7) and (8) it is obvious that for $i, j = 1, 4$, the sub-matrix $[\chi]_{ij}$ is exactly the reduced density matrix ρ_A, since on Bob's side, only the identity is evaluated. By construction, we have also $\chi = \chi^\dagger$. So we can summarize:

Observation 1 *For any bipartite state ρ, its EVM $\chi(\rho)$ (as defined in Eq.(7)) has the following properties:*

- *χ is Hermitean: $\chi = \chi^\dagger$.*
- *for $i, j = 1, 4$, the sub-matrix $[\chi]_{ij}$ is the reduced density matrix ρ_A (and thus, positive, Hermitean and of unit trace)*
- *for any projector $|s\rangle\langle s|$, the EVM $\eta_s := Tr_A\{(|s\rangle\langle s| \otimes \mathbb{1}_B)\chi\}$ of the corresponding mode must satisfy*

$$\left(\eta_s + \frac{i}{2}\tilde{J}\right) \geq 0. \tag{14}$$

This condition implies $(\eta_s - i\tilde{J}/2) \geq 0$ and $\eta_s \geq 0$ as well.

C. Separability conditions

Now we want to derive necessary conditions for separability in terms of the EVM. We will start with pure product states.

For a pure product state $\rho = |s\rangle\langle s| \otimes \rho_s$, the bipartite EVM $\chi(\rho)$ is of the form $|s\rangle\langle s| \otimes \eta_s$. Since the projector $|s\rangle\langle s|$ is positive, by virtue of Eq.(14) χ must then fulfill

$$\chi \pm \left(|s\rangle\langle s| \otimes \frac{i}{2}\tilde{J} \right) = |s\rangle\langle s| \otimes \left(\eta_s \pm \frac{i}{2}\tilde{J} \right) \geq 0\,. \quad (15)$$

For a general separable state, which can be written as $\rho = \sum_k p_k \rho_k^A \otimes \rho_k^B$, the EVM $\chi(\rho) = \sum_k p_k \rho_k^A \otimes \eta_k^B$ must hence satisfy

$$\chi \pm \left(\frac{i}{2}\rho_A \otimes \tilde{J} \right) \geq 0\,. \quad (16)$$

The second relation holds due to Eq. (15) and the fact that $\sum_k p_k \rho_k^A = \rho_A$. We can summarize:

Observation 2 *For any separable state ρ, its EVM χ additionally to the conditions specified in Observation 1 must satisfy the following inequalities:*

$$\chi \pm \frac{i}{2}\rho_A \otimes \tilde{J} \geq 0. \quad (17)$$

Note that this inequality implies $\chi \geq 0$, as well.

IV. APPLICATION TO A GENERAL PM SCHEME

Let us now connect these necessary conditions on the EVM of a bipartite separable state ρ to the knowledge on that state accessible in any PM scheme with two signal states and heterodyne detection. Given the available entries of the EVM we derive a set of matrix inequalities which have to be fulfilled. The question whether they can be fulfilled can then be solved efficiently by semidefinite programming.

A. Knowledge on χ in PM schemes

Let us first determine the entries in the EVM which are accessible in any PM scheme. For $|s\rangle_A = |0\rangle_A$ or $|1\rangle_A$, η_s corresponds to Bob's measurement outcomes under the condition that A sent signal 0 or 1. Bob has the full information on these states ρ_0 and ρ_1, i.e., all expectation values in η_0 and η_1 are fully known. With knowledge of the a priori probabilities p_0, p_1 this gives full information on χ_{ij} for $i,j = 1,2,3$ or $i,j = 4,5,6$, i.e. for the upper left and lower right 3×3-block of χ (c.f. Eq.(7)).

For $i = 1,2,3\,, j = 4,5,6$ and vice versa, the only operator product of $|0\rangle\langle 1| \otimes B$ in Eq.(7) that can be evaluated is $|0\rangle\langle 1| \otimes \mathbb{1}$ (or $|1\rangle\langle 0| \otimes \mathbb{1}$, respectively; c.f. Eq.(8)) because they are known from the reduced density matrix of Alice.

It is important to note at this point that since $\dim(\mathscr{H}_A) = 2$, we can (and will) always choose ρ_A to be real and thus have $\rho_A = \rho_A^T$ by a proper phase choice of $|0\rangle$ and $|1\rangle$. Obviously, this property holds for arbitrary signal states sent to Bob.

The remaining 16 entries χ_{ij} (for $i = 1,2,3\,, j = 4,5,6$ and vice versa with $\{i,j\} \neq \{1,4\}$) are unknown but can be further restricted by the conditions in Observation 1 to five free complex parameters.

The explicit form of χ then becomes

$$\chi = \begin{bmatrix} & & & S & a & b \\ & p_0\eta_0 & & a & c & d \\ & & & b & d & e \\ S & a^* & b^* & & & \\ a^* & c^* & d^* & & p_1\eta_1 & \\ b^* & d^* & e^* & & & \end{bmatrix} \quad (18)$$

with S abbreviating $(\rho_A)_{01}$ and $a,b,c,d,e \in \mathbb{C}$ being free complex parameters. From Observation 1, we have the following general result holding for all protocols with two signal states and heterodyne detection:

Observation 3 *Let ρ_A, η_0 and η_1 be specified by a certain set of measurement data in an arbitrary PM scheme with two signal states and heterodyne detection. If no set of parameters $a,b,c,d,e \in \mathbb{C}$ can be found such that χ as specified in Eq.(18) satisfies the inequalities (17), then the measured bipartite state ρ must have been entangled. Consequently, if such a set of parameters can be found, then the QKD protocol is insecure.*

It is possible to show that one can concentrate on real parameters a,b,c,d,e, only:

Lemma 1 *Suppose $X = \chi$ is a solution of the form (18) to a problem specified by data η_0, η_1, ρ_A. Then there exists always a real solution $\overline{X} \in \mathbb{R}^{6\times 6}$.*

Proof: Let us first show that X^T is also a solution. Since $\eta_0^T = \eta_0$ and $\eta_1^T = \eta_1$, X^T still fits to the experimental parameters. Furthermore, since we have chosen $\rho_A = \rho_A^T$, the new X^T obeys still the inequalities (17), since $\tilde{J}^T = -\tilde{J}$. But then $\overline{X} := (X + X^T)/2$ is another solution, which is real. □

Finally we show that with all knowledge available in a PM scheme, PPT entangled states cannot be distinguished from separable states:

Lemma 2 *Suppose a PPT-entangled state ρ compatible with data η_0, η_1, ρ_A, i.e. the EVM $\chi(\rho)$ is a solution to a problem as specified in Observation 3. Then there exists a separable state $\overline{\rho}$ which is also compatible with the data, i.e. whose EVM is also a solution to the same problem.*

Proof: Since ρ is PPT, ρ^{T_A} is a valid physical state, too. From the construction of the EVM (7) it can be seen immediately that the EVM of ρ^{T_A} equals $\chi^{T_A}(\rho)$, i.e., the partial transpose of the EVM χ of ρ. Furthermore, we have $\chi^{T_A} = \chi^T$. So for

$$\overline{\rho} := \frac{1}{2}(\rho + \rho^{T_A})$$

its EVM $\overline{\chi} = (\chi + \chi^{T_A})/2 = (\chi + \chi^T)/2$ is a solution to the problem specified by the data as shown in the proof of Lemma 1. Since $\overline{\rho} = \overline{\rho}^{T_A}$ and $\dim \mathscr{H}_A = 2$, $\overline{\rho}$ is separable (Theorem 2 in [23]). So the PPT-entangled state ρ and the separable state $\overline{\rho}$ are both compatible with the available data. □

B. Implementation with semi-definite programming

It is hard to find analytically a set of parameters a, b, c, d, e to a given matrix χ (18) with ρ_A, η_0, η_1 fixed so that Ineqs.(17) are indeed fulfilled. However, this task can be easily implemented and efficiently solved with semi-definite programming [24].

A semidefinite program is a convex optimization problem of the type

$$\min_x c^T x \tag{19}$$

subject to

$$F_0 + \sum_{k=1}^{N} x_k F_k \geq 0. \tag{20}$$

Here, $x \in \mathbb{R}^N$, $c \in \mathbb{R}^N$, and the F_0, F_k, $k = 1 \ldots N$ are Hermitean matrices. The matrix inequality (20) defines a convex subset in the vector space $\mathbb{R}^N$.

Optimization problems of this type have several nice properties [24]. For usual minimization problems it is impossible to guarantee that an obtained solution is really the *global* minimum. This is not the case for semidefinite programs, since here the so-called dual problem delivers a lower bound on the minimum. Under weak conditions, this lower bound coincides with the minimum, thus global optimality of a solution may be proved. Furthermore, efficient algorithms for the implementation of semidefinite programs are freely available [25–27].

To implement the constraints in Observation 3, the question of interest is whether or not there exists a solution of the form (18) to given data matrices ρ_A, η_0, η_1 which satisfies the two inequalities (17). In the language of semidefinite programming it is only of interest whether the constraints in (20) can be fulfilled. This is a so-called feasibility problem, where the objective function (19) can be ignored.

The data matrices ρ_A, η_0, η_1 are included in F_0 as well as $\pm(i/2)\rho_A \otimes \tilde{J}$, while the free real parameters a, b, c, d, e form the vector $x \in \mathbb{R}^5$. The specific form (18) of χ then determines the shape of the real symmetric matrices F_k, $k = 1 \ldots 5$. If the problem is returned infeasible, then the bipartite state must have been entangled.

In order to illustrate our method, let us choose coherent states $|\pm\alpha\rangle$ as input states. Then, we set the a priori probabilities p_0, p_1 both to 1/2 thus $S = (\rho_A)_{01}$ in Eq. (18) becomes $\exp(-2|\alpha|^2)/2$. Now, let us assume

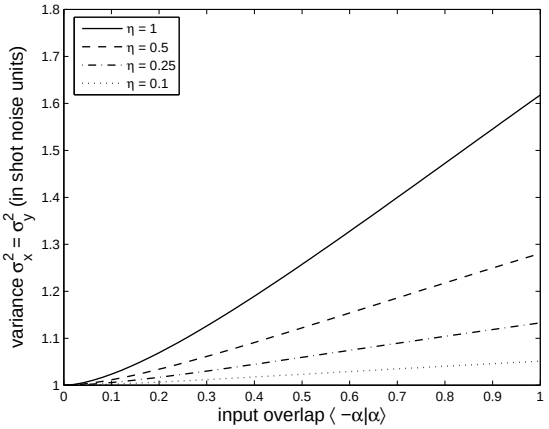

FIG. 2: Entanglement detection with semi-definite programming. For each value of transmission, the area below the corresponding line belongs to parameter pairs outcome overlap vs. quadrature variance for which entanglement can be ensured.

measurement outcomes of $\rho_{0/1}$ at Bob's site generating EVMs

$$\eta_{0/1} = \begin{bmatrix} 1 & \pm c & 0 \\ \pm c & c^2 + \sigma^2 & 0 \\ 0 & 0 & \sigma^2 \end{bmatrix} \tag{21}$$

with symmetric quadrature variances $\sigma_x^2 = \sigma_y^2$. The quadrature expectation values are set to $\langle x \rangle_{0/1} = \pm c$ and $\langle y \rangle_{0/1} = 0$. We also assume vanishing expectation values for $\mathcal{S}(xy)$. Note that this property does not necessarily mean that the outcome states ρ_0, ρ_1 are Gaussian. The performance is shown in Fig. 2 for several transmission values $\eta := c^2/|\alpha|^2$.

All lines show a similar behavior: For an input overlap $\langle -\alpha|\alpha\rangle$ close to zero, the outcome states are quite distinguishable, too. In this case, the outcomes must be extremely pure in order to show entanglement. The more the input states are overlapping, the more noise can be tolerated for a certain amount of loss.

For an overlap of 1 (i.e., $\alpha = 0$), however, the input states factorize off from Alice's logical qubits, so they are no longer entangled. Thus, in the limit of the overlap going to 1, the graph drops down to $\sigma^2 = 1$ discontinuously.

It has to be emphasized that even for 90% loss, the ability of detecting entanglement is still well within a reasonable tolerance of noise, achievable in current experiments. Also, for all transmission values η, the necessary relation between transmission and excess noise $\delta := \sigma^2 - 1$, given by $\delta < 2\eta$ [28], is satisfied.

C. Generalizations

So far we considered a scheme where we send two coherent states and perform a heterodyne measurement to

extract information about the covariance matrix and the expectation values of two quadrature operators. Any quantum mechanical measurement which allows us to infer these observable quantities will suffice to proof the presence of entanglement with our method.

One can also consider a situation where only $\langle x^2 \rangle$ and $\langle y^2 \rangle$ are measured but not $S(xy)$. This is the case when Bob measures only two conjugate quadratures by homodyne measurements. This leads to an additional free parameter f that replaces $S(xy) = 0$ in Eqn.(21). By numerical evaluation we found that the parameter regime, shown to be incompatible with separable states by our approach, is exactly the same as if we had measured $S(xy) = 0$.

Note that our analysis does not make use of the explicit form of the signal states. Instead of coherent states one could have used any two quantum mechanical states. Only the overlap between the two states is relevant and enters the analysis.

V. CONCLUSIONS

In conclusion, we have investigated separability properties of quantum states consisting of a qubit and a mode. We introduced the EVM matrix as a suitable description of such systems and derived a necessary separability criterion in this formulation. For reduced information, this separability criterion can be efficiently checked via semidefinite programming. We have then applied these results to a general PM QKD protocol using coherent signal states and heterodyne detection. Also an extension to homodyne measurement of two conjugated variables only has been given. We showed that PPT entanglement cannot be detected in this scheme. For realistic setups, however, we calculated that entanglement detection is possible even in the case of high transmission losses.

Acknowledgments

We thank Stefan Lorenz, Tobias Moroder and Volkher Scholz for valuable discussions. This work has been supported by the DFG (Emmy Noether Programm) and by the EU (OLAQUI, PROSECCO, QUPRODIS, SCALA, SECOQC) and the FWF.

[1] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).
[2] M. Curty, M. Lewenstein, and N. Lütkenhaus, Phys. Rev. Lett. **92**, 217903 (2004).
[3] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
[4] C. H. Bennett and G. Brassard, in *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India* (IEEE, New York, 1984), pp. 175–179.
[5] C. H. Bennett, Phys. Rev. Lett. **68**, 3121 (1992).
[6] M. Curty, O. Gühne, M. Lewenstein, and N. Lütkenhaus, Phys. Rev. A **71**, 022306 (2005).
[7] F. Grosshans, N. J. Cerf, J. Wenger, R. Tualle-Brouri, and P. Grangier, Quant. Inf. Comp. **3**, 535 (2003).
[8] A. M. Lance, T. Symul, V. Sharma, C. Weedbrook, and P. K. Ralph, T. C. Lam, Phys. Rev. Lett. **95**, 180503 (2005).
[9] S. K. Lorenz, N. Korolkova, and G. Leuchs, Appl. Phys. B **79**, 273 (2004).
[10] R. A. Horn and C. R. Johnson, *Matrix analyis* (Cambridge University Press, Cambridge, 1985).
[11] A. Peres, Phys. Rev. Lett. **77**, 1413 (1996).
[12] M. Horodecki, P. Horodecki, and R. Horodecki, Phys. Lett. A **223**, 1 (1996).
[13] M. Horodecki and P. Horodecki, Phys. Rev. A **59**, 4206 (1999).
[14] O. Rudolph, Phys. Rev. A **67**, 032312 (2003), see also quant-ph/0202121.
[15] K. Chen and L. Wu, Quant. Inf. Comp. **3**, 193 (2003).
[16] L. M. Duan, G. Giedke, J. I. Cirac, and P. Zoller, Phys. Rev. Lett. **84**, 2722 (2000).
[17] R. Simon, Phys. Rev. Lett. **84**, 2726 (2000).
[18] R. F. Werner and M. M. Wolf, Phys. Rev. Lett. **86**, 3658 (2001).
[19] G. Giedke, B. Kraus, M. Lewenstein, and J. I. Cirac, Phys. Rev. Lett. **87**, 167904 (2001).
[20] J. Rigas, *Detection of prepare&measure entanglement in continuous variable quantum key distribution*, Diploma thesis, University of Erlangen-Nürnberg (2005).
[21] H. P. Robertson, Phys. Rev. **46**, 794 (1934).
[22] G. Giedke, *Quantum information and continuous variable systems*, PhD Thesis, Universität Innsbruck (2001), available from `http://www.phys.ethz.ch/~giedke/publications.html`.
[23] B. Kraus, I. Cirac, S. Karnas, and M. Lewenstein, Phys. Rev. A **61**, 062302 (2000).
[24] L. Vandenberghe and S. Boyd, SIAM Review **38**, 49 (1996).
[25] J. F. Sturm, Optim. Methods Softw. **11**, 625 (1999), available from `http://sedumi.mcmaster.ca/`.
[26] K. C. Toh, M. J. Todd, and R. H. Tutuncu, Optim. Methods Softw. **11**, 545 (1999), available from `http://www.math.nus.edu.sg/~mattohkc/sdpt3.html`.
[27] J. Löfberg, in *Proceedings of the CACSD Conference* (Taipei, Taiwan, 2004), available from `http://control.ee.ethz.ch/~joloef/yalmip.php`.
[28] R. Namiki and T. Hirano, Phys. Rev. Lett. **92**, 117901 (2004).
[29] A first scheme for this task has been given in [20], though the tools developed in the present article allow a more systematical investigation.